NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

WIRELESS NETWORK SECURITY: DESIGN CONSIDERATIONS FOR AN ENTERPRISE NETWORK

by

Oh Khoon Wee

December 2004

Thesis Advisor:	Karen Burke
Thesis Co-Advisor:	Gurminder Singh

Approved for public release: distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	December 2004	Master's Thesis

4. TITLE AND SUBTITLE: Wireless Network Security: Design Considerations for an Enterprise Network	5. FUNDING NUMBERS
6. AUTHOR(S) Oh Khoon Wee	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT	12b. DISTRIBUTION CODE
Approved for public release: distribution is unlimited	

13. ABSTRACT ***(maximum 200 words)***

Since its introduction in 1999, the Institute of Electrical and Electronics Engineers (IEEE) 802.11 Wireless Local Area Network (WLAN) has become the de-facto standard for wireless networking, providing convenient and low cost connectivity. Increasingly, enterprises are extending their networks with 802.11-based WLANs to provide mobility and information-on-the-move for its employees. However, the introduction of WLANs into enterprise networks has raised major concerns about security. A poorly implemented WLAN introduces weaknesses in the enterprise network which can be exploited by attackers, resulting in severe consequences for the enterprise.

This thesis was sponsored by the DoD to study the problem of designing a secure wireless architecture for an enterprise network. The specific requirements for the enterprise network were based extensively on DoD and the intelligence community's security guidelines and policies. This thesis provides an in-depth analysis into the 802.11 standard and measures how far the standard goes in meeting the specific requirements of the enterprise network. This thesis presents a layered-defense architecture to provide a scalable design for secure wireless networks. A prototype system utilizing XML to control the flow of classified information in wireless networks is also presented.

14. SUBJECT TERMS 802.11, WLAN, 802.11i, WEP, WPA, WIRELESS	15. NUMBER OF PAGES 79
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public distribution: distribution is unlimited

WIRELESS NETWORK SECURITY: DESIGN CONSIDERATIONS FOR AN ENTERPRISE NETWORK

Oh Khoon Wee
Defense Science and Technology Agency, Singapore
B.Eng., Nanyang Technological University, 1998

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
December 2004

Author: Oh Khoon Wee

Approved by: Karen Burke
Thesis Advisor

Gurminder Singh
Co-Advisor

Peter Denning
Chairman, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Since its introduction in 1999, the Institute of Electrical and Electronics Engineers (IEEE) 802.11 Wireless Local Area Network (WLAN) has become the de-facto standard for wireless networking, providing convenient and low cost connectivity. Increasingly, enterprises are extending their networks with 802.11-based WLANs to provide mobility and information-on-the-move for its employees. However, the introduction of WLANs into enterprise networks has raised major concerns about security. A poorly implemented WLAN introduces weaknesses in the enterprise network which can be exploited by attackers, resulting in severe consequences for the enterprise.

This thesis was sponsored by the DoD to study the problem of designing a secure wireless architecture for an enterprise network. The specific requirements for the enterprise network were based extensively on DoD and the intelligence community's security guidelines and policies. This thesis provides an in-depth analysis into the 802.11 standard and measures how far the standard goes in meeting the specific requirements of the enterprise network. This thesis presents a layered-defense architecture to provide a scalable design for secure wireless networks. A prototype system utilizing XML to control the flow of classified information in wireless networks is also presented.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I wish to express my gratitude to my thesis advisors Prof Karen Burke and Prof Gurminder Singh for making this thesis possible. Thank you for your patient guidance and invaluable advice. Special thanks also to my wife Mui Hua and my daughter Hwee Shian for their love and support.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

Since its introduction in 1999, the Institute of Electrical and Electronics Engineers (IEEE) 802.11 Wireless Local Area Network (WLAN) has become the de-facto standard for wireless networking, providing mobility and connectivity at relatively low cost.

However, the key concern with the 802.11 WLANs has been security. Wireless signals can travel long distances and are not bounded by physical boundaries such as walls and perimeters. Since the Radio Frequency (RF) spectrum is a shared medium, wireless signals can also be picked up by unintended recipients such as potential attackers (with the right equipment). As noted by [Borisov 2002], when wireless signals are sent across radio waves, "interception and masquerading becomes trivial to anyone with a radio". This can compromise the confidentiality, availability and integrity of information in a network.

This thesis studies the problem of designing a secure 802.11-based wireless network architecture for an enterprise. The Department of Defense (DoD) was the main sponsor for this study, and the design of the architecture is based on requirements provided by the DoD and related intelligence agencies.

B. SCOPE

The thesis will answer the following questions, leading to the development of a wireless enterprise architecture for the DoD network:

1. What are the requirements for the DoD enterprise system?
2. How do current wireless technologies, in particular the IEEE 802.11 standard, perform with respect to the specified requirements? Are there areas of non-compliance that have to be addressed?

3. What are other supporting technologies that can be applied to better secure the network?

The specific security requirements for the DoD enterprise system were studied and analyzed. Extensive research was conducted on the IEEE 802.11 standard, focusing on the security protocols that are built-in with the 802.11 security standard, namely the Wired Equivalent Privacy (WEP), Wireless Protected Access (WPA) and the IEEE 802.11i protocols. These security protocols were analyzed in detail, and examined for compliance to the requirements for the enterprise network.

A key consideration in the design of the wireless enterprise architecture is to be able to provide defense-in-depth for the network. [NIST 2002] recommends that "the built-in security features of 802.11 (data link level encryption and authentication protocols) be used as part of an overall defense-in-depth strategy". This thesis will look further into other security mechanisms and best practices that can be built into a multi-layered defense mechanism for the wireless network.

C. REQUIREMENTS OVERVIEW

The primary aim of this thesis is to design an enterprise architecture for specific security requirements for **Confidentiality**, **Integrity** and **Availability**. Since the DoD's goal was to use this enterprise architecture in Sensitive Compartmented Information Facilities (SCIF) or by organizations processing intelligence information, the enterprise architecture must comply with the Director of Central Intelligence Directives (DCID). The specific requirements that are used in this thesis are found in the following documents:

- DCID 6/3 Manual, "Protecting Sensitive Compartmented Information within Information Systems"
- DCID 6/9 Manual, "Physical Security Standards for Compartmented Information Facilities"

For this study, we assume that Level of Concern for Confidentiality to be HIGH with Protection Level 1 required. The Levels of Concern for Integrity and Availability are assumed to be MEDIUM. The highest level of data that will be processed within the enterprise network is restricted to “UNCLASSIFIED For Official Use Only”.

D. DESIGN STRATEGY

The strategy for the design of the enterprise architecture takes into consideration the following factors. In the current state of the art in wireless technology, wireless networks are less secure compared to wired networks and the data throughput supported in wireless networks is also often significantly lower. Based on the security and performance considerations, it is not practical to design a pure wireless network system for the enterprise. Furthermore, most enterprises already deploy extensive wired networks, and considerable effort has been spent to secure these networks. This strategy proposes a hybrid solution in which the wireless network is designed to extend the services of an existing wired network. The key points of the strategy is illustrated in Figure 1 and discussed below.

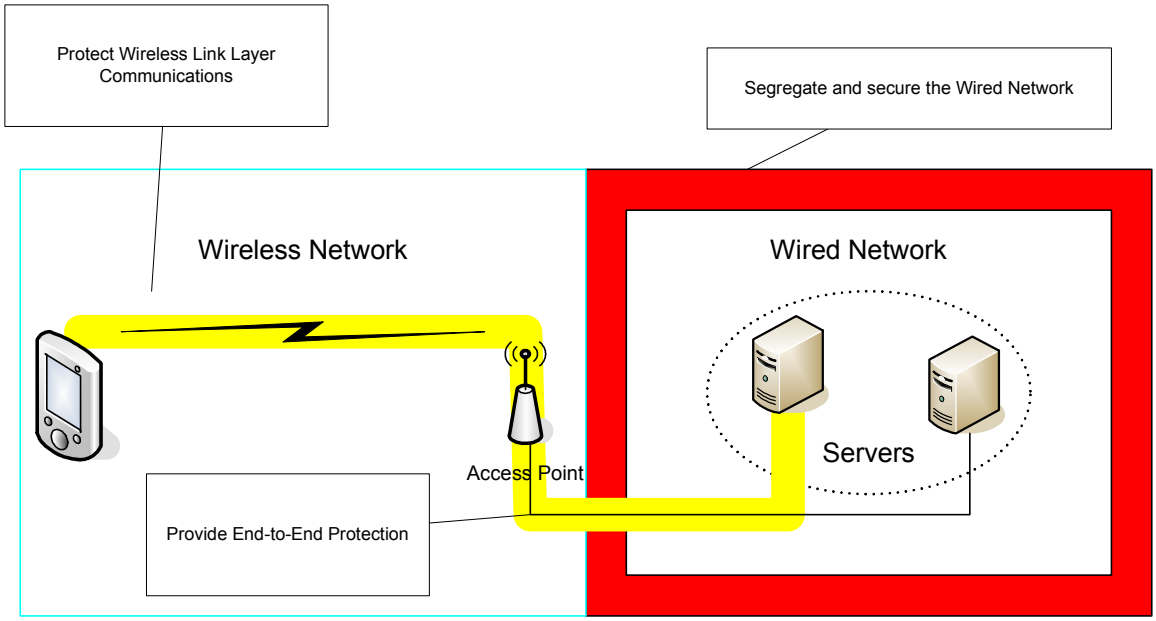

Figure 1. Design Strategy

1. Segregate and secure the wired network. This involves building a strong defensive perimeter around the boundary of the wired network, and hosting the mission critical computers and servers within the wired network. Standard techniques such as using firewalls and intrusion detection tools can be applied. Since the techniques to secure wired networks are well known, they will not be further discussed in this report.

2. Deploy the wireless infrastructure outside the perimeter of the wired network. This will prevent inherent weaknesses in WLAN security from creating vulnerabilities in the defensive perimeter of the wired network.

3. Protect the RF links used to carry information from between access points and the mobile device. The link has to be secured to protect information and data that is transmitted over the airwaves. In this study, we will focus on the link layer WEP, WPA and the 802.11i protocols.

4. Provide end to end security between hosts in the wired and wireless networks. Note that link layer only protects data packets in transit

over the RF medium. By providing end-to-end security, data in transit will be protected over the wired and wireless networks.

E. THESIS ORGANIZATION

Chapter II provides an overview of the DCID specifications and an analysis of the specific requirements that are applicable to the wireless network architecture

Chapter III will focus on the protection of the wireless links between the mobile nodes and the wireless infrastructure. This chapter provides a detailed description of the key protocols used in 802.11 to provide link protection, namely the WEP, WPA and the IEEE 802.11i protocols.

Chapter IV studies the security mechanisms that can be built over the IEEE 802.11 standard to provide end-to-end protection, and provide a strong layered-defense architecture for the network. This chapter also provides a description of an access control prototype that can be used to control the flow of sensitive information in the enterprise network.

Finally, Chapter V concludes the findings of this thesis, and provides recommendations for subsequent research work in the area of wireless security.

THIS PAGE INTENTIONALLY LEFT BLANK

II. REQUIREMENTS

This chapter provides an overview of the requirements that were specified for the enterprise architecture. The requirements were based extensively on the Director Of Central Intelligence Agency Directives (DCID) 6/3 and 6/9 documents. This chapter focuses on the relevant requirements that are applicable to the wireless network, and is not intended to provide a comprehensive study of the abovementioned DCID documents. For additional details, refer to [DCID 6/3 1999] and [DCID 6/9 2002].

A. DCID 6/9 "PHYSICAL SECURITY STANDARDS FOR COMPARTMENTED INFORMATION FACILITIES"

The DCID 6/9 manual establishes the physical security standards to govern the construction and protection of facilities for storing, processing and discussing Sensitive Compartmented Information (SCI) which requires extraordinary safeguards. The focus of DCID 6/9 is to provide physical protection requirements for SCIFs, with the intention to prevent as well as detect visual, acoustical, technical, and physical access by unauthorized persons. Detailed specifications on the physical controls and the construction criteria required for a SCIF are provided.

For the most part, the DCID 6/9 manual is concerned with the construction and physical security of facilities that are used to house SCI. The sections that are related to the use of wireless technologies are Annex D Part I which provides guidelines on the use of electronic equipment in SCIFs, and Annex G which covers the approval process required for the deployment of wireless technologies in SCIFs.

B. DCID 6/3 "PROTECTING SENSITIVE COMPARTMENTED INFORMATION WITHIN INFORMATION SYSTEMS"

The DCID 6/3 manual provides policy guidance and requirements for the protection of SCI stored or processed on an Information System (IS). An IS is defined as any telecommunications and/or computer related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data. DCID 6/3 applies to all United States Government departments and agencies, their contractors and allied governments processing intelligence information.

The DCID 6/3 manual defines the concepts of *Level of Concern* and *Protection Level*, and provides guidance on how to use these concepts to determine the appropriate technical security requirements for confidentiality, integrity and availability that each IS must meet.

1. Level-of-Concern

The DCID 6/3 manual defines Level-of-Concern as a rating assigned to an IS. A separate Level-of-Concern is assigned for confidentiality, integrity and availability, and this can be BASIC, MEDIUM, or HIGH.

The Level-of-Concern assigned to an IS for confidentiality is based on the sensitivity of the information it maintains, processes, and transmits. By definition, any system that processes intelligence information requires a HIGH Level-of-Concern rating. MEDIUM and BASIC levels of concern are not applicable to confidentiality, since any system that is accredited by the DCID 6/3 by definition processes intelligence information. Since the architecture discussed in this paper is accredited under the DCID 6/3 manual, it is assigned a HIGH confidentiality Level-of-Concern.

The Level-of-Concern assigned to an IS for integrity is based on the degree of resistance to unauthorized modifications. The Level-of-Concern assigned to an IS for availability is based on the needed availability of the

information maintained, processed and transmitted by the system for mission accomplishment, and how much tolerance for delay is allowed.

Table 1 provides a summary of the indicators for Confidentiality, Integrity and Availability for the various Levels-of-Concern.

Level of Concern	Confidentiality Indicators	Integrity Indicators	Availability Indicators
BASIC	Not applicable to DCID 6/3	Reasonable degree of resistance required against unauthorized modification, or loss of integrity will have an adverse effect	Information must be available with flexible tolerance for delay, or loss of availability will have an adverse effect
MEDIUM	Not applicable to DCID 6/3	High degree of resistance required against unauthorized modification, or bodily injury might result from loss of integrity, or loss of integrity will have an adverse effect on organizational-level interests.	Information must be readily available with minimum tolerance for delay, or bodily injury might result from loss of availability, or loss of availability will have an adverse effect on organizational-level interests.
HIGH	All Information protecting intelligence sources, methods and analytical procedures. All Sensitive Compartmented Information	Very high degree of resistance required against unauthorized modification, or loss of life might result from loss of integrity, or loss of integrity will have an adverse effect on national-level interests, or loss of integrity will have an adverse effect on confidentiality.	Information must always be available upon request, with no tolerance for delay, or loss of life might result from loss of availability, or loss of availability will have an adverse effect on national level interests, or loss of availability will have an adverse effect on confidentiality.

Table 1. Summary of Key Indicators for Confidentiality, Integrity and Availability for Various *Levels-of-Concern* [DCID 6/3 1999]

2. Protection Level

The DCID 6/3 manual defines Protection Level as an “indication of the implicit level of trust that is placed in a system’s technical capabilities”. The concept of Protection Level is applicable only to confidentiality. A Protection Level is determined based on the classification and sensitivity of information processed on the system, relative to the clearance(s), formal access approval(s) and need-to-know of all direct and indirect users that receive information from the IS without manual intervention and reliable human review.

The DCID 6/3 manual specifies 5 different Protection Levels, ranging from PL1 to PL5, and the criteria for selecting the suitable Protection Levels for an IS is shown in Table 2.

Protection Level	Criteria
PL 1	An IS operates at Protection Level 1 when all users have all required approvals for access to all information on the IS. This means that all users have all required clearances, formal access approvals, and the need to know for all information on the IS.
PL 2	An IS operates at Protection Level 2 when all users have all required formal approvals for access to all information on the IS, but at least one user lacks administrative approval for some of the information on the IS, This means that all users have all required clearances and all required formal access approvals, but at least one user lacks the need to know for some of the information on the IS.
PL 3	An IS operates at Protection Level 3 when at least one user lacks at least one required formal approval for access to all information on the IS. This means that all users have all required clearances, but at least one user lacks formal access approval for some of the information on the IS.
PL 4	An IS operates at Protection Level 4 when at least one user lacks sufficient clearance for access to some of the information on the IS, but all users have at least a SECRET clearance.
PL 5	An IS operates at Protection Level 5 when at least one user lacks any clearance for access to some of the information on the IS.

Table 2. Selection Criteria for Protection Levels [DCID 6/3 1999]

C. SPECIFIC REQUIREMENTS

The broad requirements for specified by the DoD for the areas of Confidentiality, Integrity and Availability are as follows:

Confidentiality: Level-of-Concern **HIGH**, Protection Level 1 (PL1)

Integrity: Level-of-Concern **MEDIUM**

Availability: Level-of-Concern **MEDIUM**

Based on the Level-of-Concern and Protection Level required, the policies that are applicable to the design of the wireless enterprise architecture are extracted. These are tabulated and shown in Table 3.

POLICY	REFERENCE
CONFIDENTIALITY (Level of Concern: HIGH, PL1)	
Data Storage Information encrypted using NSA-approved encryption mechanisms appropriate for the classification of stored data	DCID 6/3 4.B.1.a(7)(d)
Data Transmission Information distributed using NSA-approved encryption mechanisms appropriate for the classification of the information	DCID 6/3 4.B.1.a(8)(a)(3)
Identification and Authentication An identification and authentication (I&A) management mechanism that ensures a unique identifier for each user and that associates that identifier with auditable actions taken by the user	DCID 6/3 4.B.1.b(3)
Identification and Authentication Access to the IS by privileged users who either reside outside of the IS's perimeter or whose communications traverse data links(extranets, INTERNET, phone links) that are outside of the IS's perimeter shall require the use of strong authentication (i.e., an I&A technique that is resistant to replay attacks)	DCID 6/3 4.B.1.b(4)
INTEGRITY (Level of Concern: MEDIUM)	
Protect against unauthorized modification/tampering of data in transit over the wireless medium	

Table 3. Specific Requirements for the Wireless Enterprise

D. REQUIREMENTS FOR AVAILABILITY

The policies and requirements shown in Table 3 are focused on the areas of confidentiality and integrity. For the area of Availability with MEDIUM level of concern, the DCID 6/3 manual specifies that adequate processes and procedures to allow for the restoration of a system in the event of a failure. DCID 6/3 also requires the implementation of "communications capability that provides adequate communications to accomplish the mission when the primary operations communications capabilities are unavailable" [DCID 6/3 1999, Section 6.B.2.a(4)].

The requirements for availability are addressed by providing sufficient redundancy and back-ups in the wired and wireless networks. In fact, the redundancy design should be focused on the wired domain, since this is where the mission critical servers and computers will be located. On the wireless domain, provide sufficient spare network capacity which can be activated in the event of a network failure. Mission critical functionalities provided in the wireless network should also be replicated in the wired network. These measures will provide continued mission capability in the event of a failure in the wireless domain.

III. IEEE 802.11: LINK SECURITY MECHANISMS

This chapter examines the different link layer security protocols that are provided in the IEEE 802.11 WLAN standard. (A simple overview of the 802.11 standard is provided in Appendix A). The purpose of these protocols is to protect communications traveling over airwaves between mobile nodes and access points, and prevent unauthorized access to information on the network.

In this chapter, we will first study the WEP protocol and look into its well-publicized weaknesses. This will be followed by an analysis of the protocols that were developed to replace WEP, specifically the IEEE 802.1x Port-Based authentication, WPA and the IEEE 802.11i protocols. An evaluation and comparison of these protocols will be made with respect to the requirements of the enterprise network.

A. WIRED EQUIVALENT PRIVACY (WEP)

The IEEE 802.11 standard specifies a security standard known as WEP to provide security for the wireless network. A detailed discussion on the WEP is provided to give a better understanding of its limitations, and how these limitations will eventually be remedied by the WPA and IEEE 802.11i protocols.

WEP was designed to provide security on the wireless network at a level equivalent to wired networks. The 3 main security goals for WEP are: [Borisov 2002]:

- **Confidentiality**: Prevent eavesdropping by using an encryption scheme based on the RC4 stream cipher.
- **Access Control**: Protect access to a wireless network infrastructure by requiring users to demonstrate knowledge of a shared secret key k (more commonly known as the WEP key). This key is shared among all legitimate users of the WLAN network.

- **Data Integrity**: To prevent tampering of the transmitted messages, through a CRC-32 checksum.

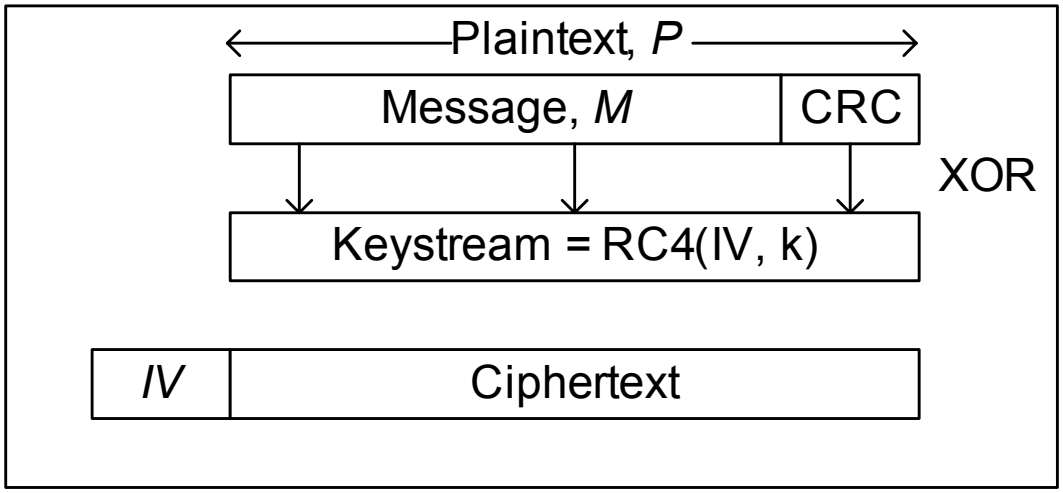

Figure 2. WEP Encryption Process

A description of the encryption process used in WEP is shown in Figure 2. We assume that the user has the correct secret key *k* to access the network. The process to encrypt a user generated message M is as follows:

Step 1: A 32 bit Cyclic Redundancy Checksum (CRC) is computed for the message M. The CRC is appended with message M to form the plaintext message P.

Step 2: A RC4 keystream is generated using the secret key k and an Initialization Vector (IV) as inputs. The IV is used to ensure that subsequent data packets are encrypted with different keystreams, even though the same secret key is used.

Step 3: The RC4 keystream is EXCLUSIVE-ORed (XOR) with the plaintext message P, to generate the ciphertext C.

Step 4: The IV is concatenated with the ciphertext, and the entire frame is transmitted. The IV is not encrypted and is transmitted in the clear.

Step 5: When the message frame arrives at the recipient (another host on the wireless network also possessing the secret key k), the IV is extracted from

the frame. The IV is used together with the shared secret key k to generate the original RC4 keystream. The original plaintext P is then recovered by performing an XOR of the ciphertext and keystream.

Step 6: The recipient host performs an integrity check by computing the checksum for the received message, and comparing it with the received CRC checksum. The message passes the integrity check if the 2 checksums are identical. If the checksums are different, the message is considered to be compromised and will be discarded.

Table 4 provides a summary of the various parameters used in the WEP mechanism

PARAMETER	PROPERTIES
Secret key, k (aka WEP key)	40 bits (used in early versions of WEP) 104 bits (current standard)
Initialization Vector, IV	24 bits
Integrity Checksum	32 bit CRC
Encryption Algorithm	RC4 Stream Cipher

Table 4. Specifications of Key Parameters used in WEP

B. WEAKNESSES OF WEP

The WEP mechanism came under intense scrutiny over the past few years due to its inherent security flaws. [Borisov 2002] demonstrated that WEP falls short of achieving its security goals for confidentiality, integrity and access control. Based on their research, WEP was found to be insecure due to improper implementation of the RC4 algorithm and the use of the CRC 32 checksum for data integrity. The key issues with WEP are summarized as follows:

1. Integrity

The CRC 32 checksum does not provide strong message integrity. It was shown that an attacker can modify the contents of a message packet as well as the corresponding CRC-32 checksum even without knowing the secret encryption key.

2. Authentication

The authentication mechanism used in WEP is a simple “challenge and response” scheme based on whether a user has knowledge of a shared secret. In the case of WEP, this shared secret is the WEP key that is shared among all users of the wireless network. The problem with using WEP authentication is that users cannot be individually identified and authenticated, since anyone with the WEP key will be granted access.

Another issue with WEP is that it does not support mutual authentication. Hence a user cannot challenge and authenticate a network access point, and cannot be assured that it is connecting to a legitimate network.

3. Confidentiality

WEP does not protect confidentiality due to improper implementation of the RC4 algorithm in the WEP protocol. Poor key management, as well as the reuse of IV can allow attackers to break the WEP key if sufficient packets are sniffed and collected off the airwaves. Once the WEP key is broken, decrypting information carried on the wireless network becomes a trivial affair. Tools have been developed that exploit the weaknesses in WEP and these can be freely downloaded via the Internet. Examples of such tools are AirSnort (available at http://airsnort.shmoo.com) and WEPCrack (available at http://wepcrack.sourceforge.net).

C. IEEE 802.1X

The IEEE 802.1x is a port based protocol that provides authentication and authorization for both wired and wireless networks. It was included in the 802.11 standard to remedy the weaknesses in the authentication processes used in WEP. IEEE 802.1x was ratified in Jun 2001, and is currently supported in many 802.11 cards and access points. (The full specification is available at http://www.ieee802.org/1/pages/802.1x.html).

1. Principle of Operation

802.1x defines three entities in the authentication process [Edney and Arbaugh 2004]:

- Supplicant - entity that wants to join a network i.e. a wireless client.
- Authenticator - entity that controls access to the network. In the case of WLANs, this refers to an access point.
- Authentication server - entity that makes the authorization decisions.

A general overview of the authentication process used in 802.1x is illustrated in Figure 3.

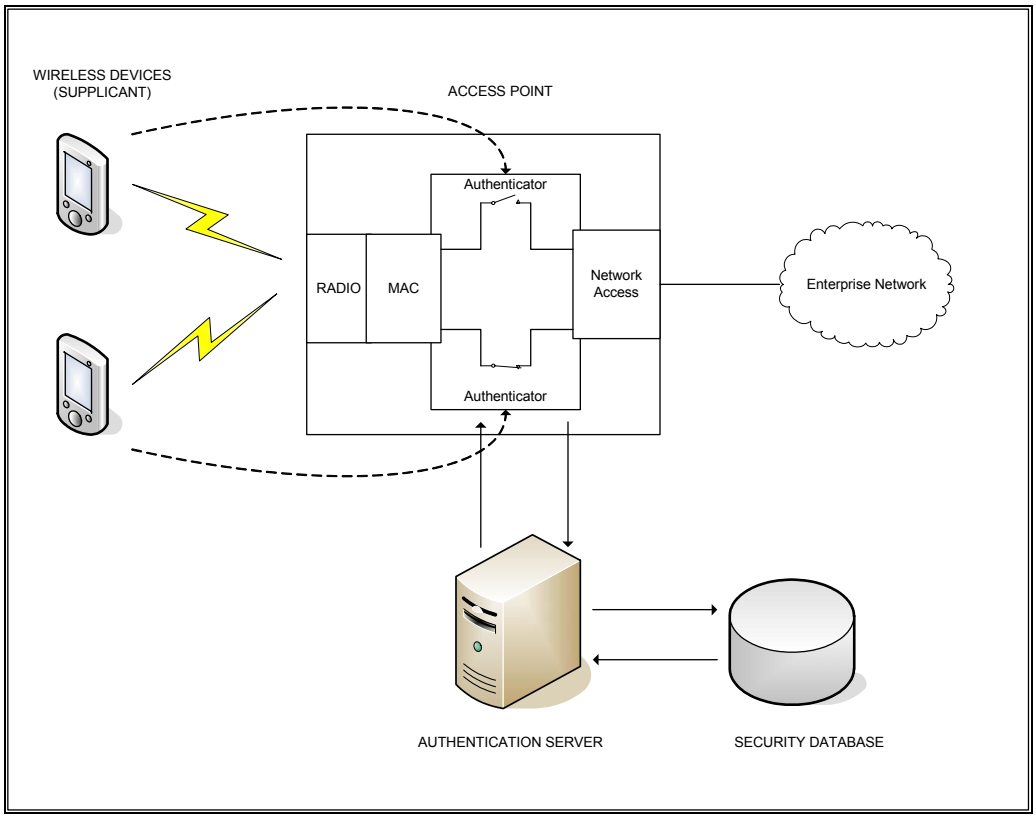

Figure 3. Overview of 802.1x Authentication Protocol (from [Edney & Arbaugh 2004])

In Figure 3, an authenticator is created together with a logical port for each supplicant requesting access to the network. The authenticator controls access to network resources by using manipulating logical switches within the access point. By default, the logical switches are in the open position. A wireless device has to submit credentials (such as user ID and a password) to the authenticator, which in turn relays these messages to the authentication server. The authentication server uses the credentials provided by the wireless device and determines if access is to be granted. If access is granted, the logical switch controlling the connection for that wireless device will be closed thereby enabling access to the network.

2. Extensible Authentication Protocol (EAP)

802.1x is intended to provide strong authentication, access control and key management control, which is not provided in WEP. 802.1x is based on EAP or more specifically EAP over Local Area Networks (EAPOL). EAP is general messaging protocol that provides communications and message exchanges between different parties in the authentication process. Note that EAP does not specify the type of authentication method used. However, different authentication methods have been implemented to work with EAP, including Kerberos, public/private keys, as well as biometrics. For a full listing of EAP authentication methods, refer to [Bersani 2004].

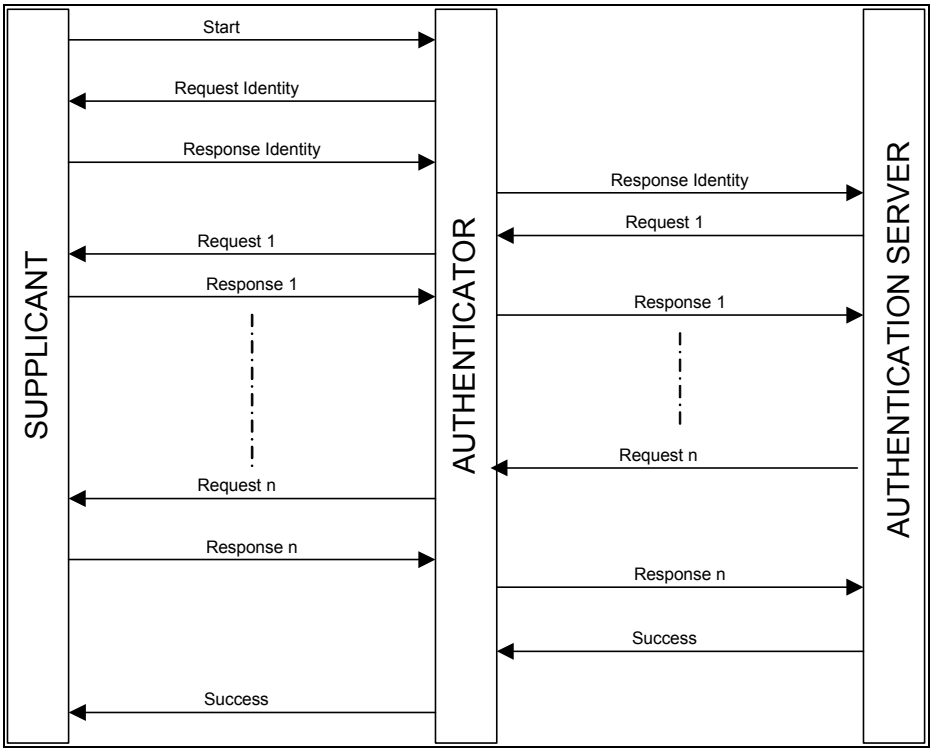

Figure 4. General EAP Message Flow in Authentication Process (from [Edney & Arbaugh 2004])

The general authentication sequence using EAP is shown in Figure 4. A supplicant starts the authentication process by sending an EAP-Start message to the authenticator. On receiving the EAP-Start message, the authenticator

responds with an EAP Request Identity message to determine the identity of the supplicant. The supplicant follows up by sending its identify information using the EAP Response Identity message which is forwarded by the authenticator to the authentication server. The authentication server initiates a series of challenges to the supplicant, which provides responses to each challenge. The authentication server checks the responses received from the supplicant, and returns a Success message to the authenticator if the responses are correct. On receiving the Success message from the authentication server, the authenticator grants access to the supplicant.

Most current applications use the EAP-TLS method (one of the EAP methods) for authentication with an authentication server. EAP-TLS (EAP-Tunneled Layer Security) uses a certificate-based mechanism to perform mutual authentication and key exchange, and is generally considered to be the strongest EAP method. Since EAP-TLS uses certificates, PKI must be supported in the enterprise network. The authentication server is usually a RADIUS-based server. However, 802.1x does not specify RADIUS as the default authentication server, and other authentication servers can be used as long as the servers support EAP.

D. WI-FI PROTECTED ACCESS

The Wi-Fi Protected Access (WPA) is a standards based, interoperable security specification developed by the Wi-Fi Alliance. The goal of WPA is to provide intermediary fixes to the vulnerabilities of WEP. Existing 802.11 network equipment can be upgraded to WPA through software or firmware upgrades.

The key features of WPA are as follows:

1. Temporal Key Integrity Protocol (TKIP)

TKIP is designed to address WEP's weaknesses in data encryption. As discussed in the earlier sections, the current WEP implementation uses a static shared secret key together with a short (24 bit) initialization vector to generate the encryption keystream using the RC4 algorithm.

TKIP continues to use the RC4 algorithm for data packet encryption. However, unlike WEP which uses a static shared secret key, TKIP uses a temporal key that is changed every 10000 packets. A longer 48 bit initialization vector is also adopted to prevent the reuse of initialization vectors over the life-time of a temporal key. These measures make it much more difficult for potential attackers to break the TKIP key using existing WEP-breaking techniques.

2. Michael Message Integrity Check

The Michael Message Integrity Check (MIC) is intended to provide protection data in transit against unauthorized modifications or tampering. The Michael algorithm uses a cryptographic digest of the original message as an integrity checksum. This protects the integrity of data packets on the wireless networks, since any attempt to modify packets will be detected.

However, one important consideration in the design of WPA was to be able to operate on existing 802.11 devices with low CPU capacity. With the constraints of CPU power, it is not feasible to design the Michael MIC to provide the same level of security as other integrity checksums such as MD5. In view of this weakness, TKIP implements additional countermeasures to work with the Michael MIC. Specifically, when an access point detects two packets that have failed the Michael algorithm on a particular temporal key, it will drop the association, generate new keys and wait for a minute before creating a new association to the host.

A concern with the TKIP countermeasures is that attackers can launch a denial of service attack by flooding access points with messages that have corrupted integrity checksums. This can result in repeated time-outs at the access points (for up to one minute each time), and thereby deny legitimate users from access to the network.

However, this risk of a possible denial of service attack should be weighed against the alternatives of WEP (which is fundamentally broken) or having no security mechanism at all. In the latter cases, an attacker can gain unrestricted access to the network and inflict damage while remaining undetected. In the case of WPA, network monitoring tools can be programmed to look out for frequent time-outs at access points which would indicate an active attack. This could provide responsive detection and execution of contingency plans to contain an attack.

E. IEEE 802.11I

The IEEE 802.11i standard was developed by the IEEE as a replacement for the flawed WEP protocol. The protocol was recently ratified by IEEE in May 04, and first products supporting 802.11i are expected to be on the market in the early part of 2005.

IEEE 802.11i is designed to be compatible with the WPA protocol. 802.11i supports TKIP encryption and the Michael Message Integrity Check used in WPA, as well as the 802.1x protocol for authentication. However, it should be noted that TKIP is built around the flawed implementation of the RC4 encryption algorithm in WEP, and is therefore considered to be an interim solution for encryption security.

To counter the weaknesses in the RC4-based encryption, 802.11i introduces 2 additional encryption protocols based on the FIPS-approved Advanced Encryption Standard (AES) algorithm.

1. Counter Mode with CBC-MAC Protocol (CCMP)

CCMP is the mandated encryption technique in the 802.11i standard. It employs the AES algorithm using the CCM mode of operation. CCM utilizes the Counter Mode (CTR) for data encryption and Cipher Block Chaining Message Authentication Code (CBC-MAC) to ensure message authenticity and integrity.

CCMP uses the CTR mode in AES to encrypt data for transmission. The basic mechanism for AES CTR mode encryption is shown in Figure 5 below.

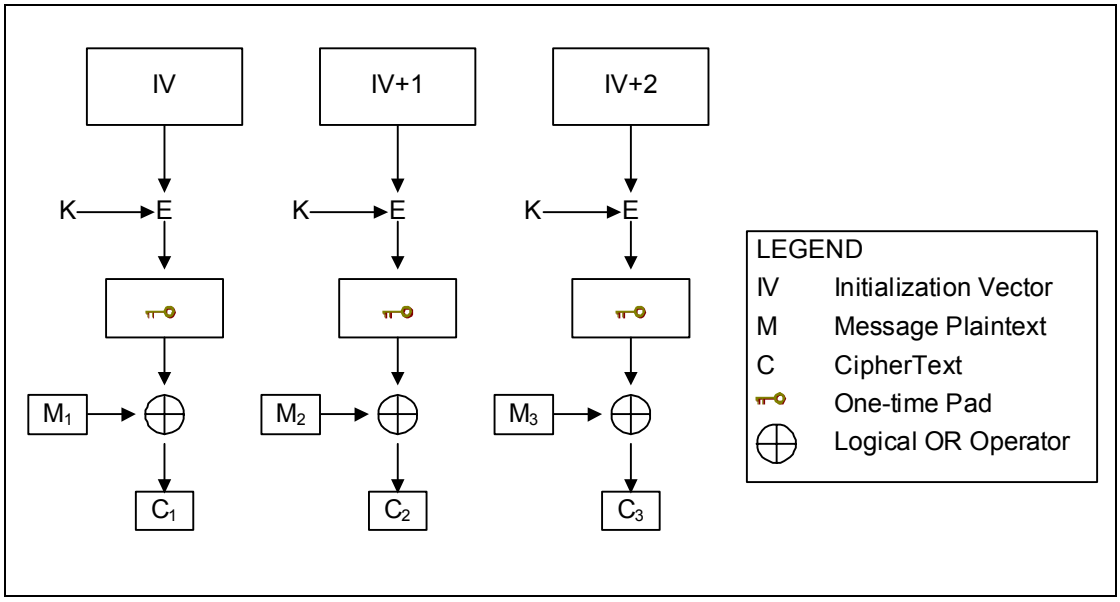

Figure 5. AES Counter (CTR) Mode Encryption Process (from [Kaufman 2002])

A 128 bit temporal key (K) together with a 48 bit IV is used to generate a one-time pad using the AES algorithm (E). The IV is incremented after generating each one-time pad. A logical OR operation is then performed with the message plaintext and the corresponding one-time pad.

The advantage of using CTR mode is that it provides equivalent encryption security compared with other AES modes but is computationally less intensive. In CTR mode, the one-time pads can be pre-computed for a given temporal key, and the encryption is a simple logical OR operation. Since chaining is not employed in CTR mode, message packets can be decrypted independently

of previous message packets. However, the encryption process will be weakened if the same key and IV is used to encrypt different messages (this is the problem faced in WEP). To tackle this, the temporal key has to be refreshed periodically via the 802.1x protocol, and a longer 48 bit IV is used to prevent the IV collisions over the active life time of each temporal key.

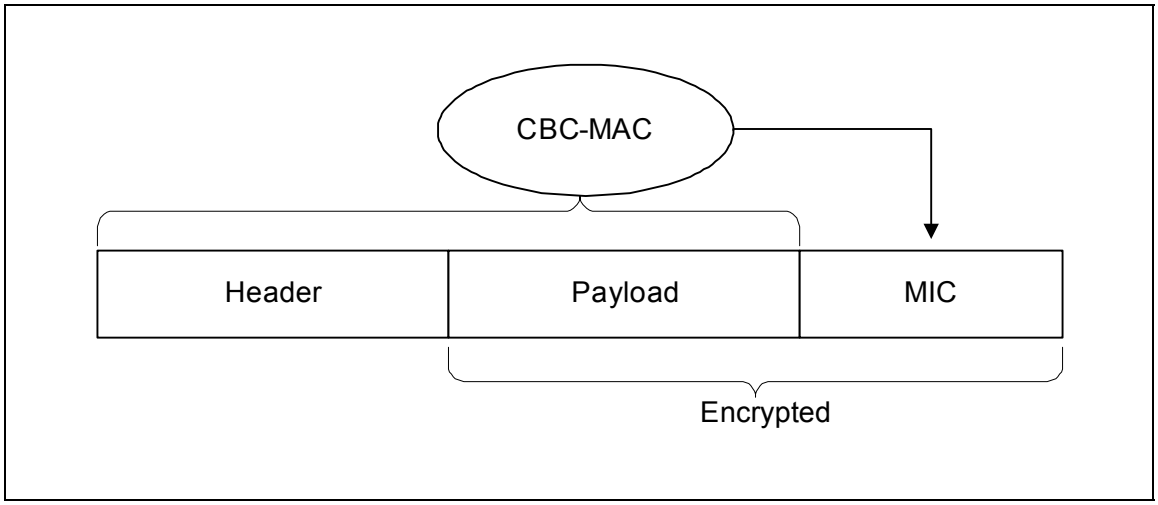

Figure 6. Message Integrity Check using CBC-MAC Computation

To provide data integrity, a message integrity check (MIC) is generated for each message packet using CBC-MAC. This is illustrated in Figure 6. The MIC is computed over the payload and the header, and the resulting MIC is appended. Encryption is then applied over the payload and the MIC, while the header is sent in the clear. Since the header is included in the computation of the MIC, any unauthorized modification or corruption of the header will also be detected. This prevents attackers from spoofing data packets on the network.

2. WRAP

WRAP was the original AES-based proposal for 802.11i encryption. This protocol is based on AES in the OCB (Output Feedback) mode. WRAP was replaced by CCMP due to intellectual property rights issues, but it was kept in the 802.11i draft as some vendors had already implemented WRAP modules in their hardware.

A summary of the key features of WEP, WPA and 802.11i is provided in Table 5. (For details on the AES algorithm, refer to [FIPS197 2001])

Key Features	**WEP**	**WPA**	**802.11i**
Encryption Algorithm	RC4	RC4	CCMP (using AES CCM)
Key Size	40 or 104 bits	2 keys used 128 bits key for encryption 64 bit key for authenticity and integrity checking	128 bits
Initialization Vector	24 bit	48 bit	48 bit
Integrity Check	32 bit CRC	Michael MIC	CBC-MAC
Authentication and Key Management	None	EAP-based using 802.1x	EAP-based using 802.1x

Table 5. Comparison of WEP, WPA and IEEE 802.11i Security Protocols

F. REQUIREMENTS MATRIX

Table 6 provides a summary of WEP, WPA and 802.11i versus the requirements specified in the DCID documents.

REQUIREMENTS		WEP (Compliant/Not compliant)	WPA (Compliant/Not compliant)	IEEE 802.11i (Compliant/Not compliant)
CONFIDENTIALITY (Level of Concern: HIGH, PL1)				
Data Storage Information encrypted using NSA-approved encryption mechanisms appropriate for the classification of stored data	DCID 6/3 4.B.1.a(7)(d)	Not compliant	Not compliant	Compliant (a minimal 128 bit key length is required) AES-encryption is approved by the Committee On National Security Systems, for systems handling information up to SECRET classification.
Data Transmission Information distributed using NSA-approved encryption mechanisms appropriate for the classification of the information	DCID 6/3 4.B.1.a(8)(a)(3)	Not compliant	Not compliant	Compliant
Identification and Authentication An identification and authentication (I&A) management mechanism that ensures a unique identifier for each user and that associates that identifier with auditable actions taken by the user	DCID 6/3 4.B.1.b(3)	Not compliant. Does not provide means to uniquely identify a user	Compliant 802.1x mechanism to provide unique user identification and authentication.	Compliant 802.1x mechanism to provide unique user identification and authentication.

Identification and Authentication Access to the IS by privileged users who either reside outside of the IS's perimeter or whose communications traverse data links(extranets, INTERNET, phone links) that are outside of the IS's perimeter shall require the use of strong authentication (i.e., an I&A technique that is resistant to replay attacks)	DCID 6/3 4.B.1.b(4)	Not compliant Does not provide strong authentication measures	Compliant Strong authentication can be implemented with 802.1x	Compliant Strong authentication can be implemented with 802.1x
INTEGRITY (Level Of Concern: MEDIUM)				
Protect against unauthorized modification/tampering of data in transit over the wireless medium		Not compliant. WEP integrity checksum can be tampered without detection	Not Compliant Concern over denial of service attack with Michael MIC	Compliant CBC-MAC integrity check

Table 6. Comparison of WEP, WPA and 802.11i Security Functions Versus DCID requirements

G. COMPARISON AND RECOMMENDATIONS

Comparing the performances of WPA, 802.11i and the WEP protocols in Table 6, we observe that 802.11i is the only protocol that satisfies all the listed requirements in the table. 802.11i adopts AES encryption which is approved by the National Institute of Standards and Technology (NIST) for use in government applications. More importantly, AES is approved by the National Security Agency for use in protecting classified information up to the SECRET level [CNSS 2003], provided that encryption keys of at least 128 bits are used. Furthermore, the CBC-MAC integrity protection is not susceptible to denial-of-service attacks as compared to the Michael implementation in WPA.

There are some issues that need to be considered when deciding to adopt the 802.11i standard in the enterprise architecture. 802.11i requires additional

hardware co-processors in order to support AES encryption, and these co-processors are not available in current 802.11 NICs and access points. Hence, extensive hardware upgrades/replacement is required to upgrade current networks to 802.11i standard. However, 802.11i-compliant products are only expected to emerge in the market in early 2005. In the meantime, it is recommended that current 802.11 networks are upgraded to WPA standard

The recommendations with regards to 802.11i and WPA are as follows:

1. Evaluate and adopt 802.11i when it becomes available. 802.11i currently provides the best security among the 802.11 security protocols.

2. In the mean time, all wireless network equipment should be updated to WPA standard. Current 802.11 network equipment can be upgraded to WPA standard via a software or firmware upgrade.

3. When evaluating 802.11i products, verify that these support at least 128-bit encryption keys, which is the minimum key length required for AES to be used in a network with SECRET classification. 802.11i products that support longer encryption keys (192-bits, 256-bits etc) can be used in networks with classification of up to TOP SECRET. It is useful also to verify that the different key lengths can be selected to match the corresponding security classification of the network.

4. Regardless of WPA or 802.11i, additional layers of defense should be built over the link layer defense mechanism to provide enhanced security. The next chapter will discuss some these additional defense mechanisms that can be included in the wireless architecture.

IV. ENTERPRISE ARCHITECTURE DESIGN

A. OVERVIEW

In the preceding chapter, we studied the WEP, WPA and 802.11i link layer protocols provided in the IEEE 802.11 standard. In this chapter, we will look at other security mechanisms and implementations that can be built on top of 802.11 link security to provide a strong, multi-layered defense architecture. The objective of a multi-layered defense architecture is to provide defense in depth, such that the failure of a particular defense mechanism will not compromise the defenses of the entire network. It will also provide flexibility and scalability in the design, whereby layers can be added or removed to suit the specific needs of a particular network.

B. VIRTUAL PRIVATE NETWORKS

Virtual Private Networks (VPN) are commonly used by enterprises to allow users to access enterprise network resources securely over a public network infrastructure. In general, VPNs employ encryption and encapsulation techniques to create a virtual tunnel that supports secure data communications over a non-secure network. However the specific encryption and encapsulation methods employed vary from vendor to vendor.

Most existing VPN implementations are based on the IPSec security protocol. IPSec provides data encryption using the 3-DES encryption algorithm. There are also VPN implementations that adopt AES and other encryption algorithms. In the context of this thesis, a VPN implementation using AES encryption (with at least 128 bit key) is recommended to satisfy the confidentiality requirements of the enterprise system.

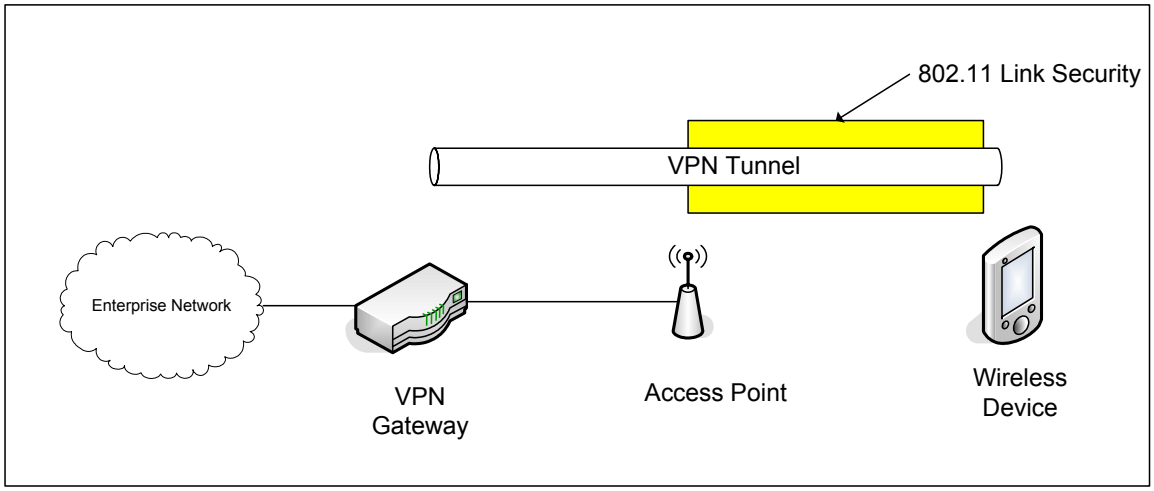

Figure 7. Integration of VPN with Wireless Network Architecture

Figure 7 illustrates the integration of VPNs for the typical wireless network. A VPN gateway is deployed at the edge of the enterprise network, and all wireless clients will have to connect via the VPN gateway in order to access the enterprise network resources. A VPN tunnel is created from the VPN gateway, through the wireless access point and terminating at the wireless client. Data packets transmitted along this path will be protected by the VPN tunnel. Implementing 802.11i link security will add additional protection along the tunnel between the access point and the wireless device. Hence any attacker attempting to infiltrate via the wireless network will have to break 2 strong layers of defenses, the 802.11i link protection and the VPN tunnel.

C. APPLICATION ENCRYPTION

In applications that require higher levels of protection, the use of encryption should be considered to protect the confidentiality and integrity of data traveling from sender to receiver. While VPNs and 802.11 link security mechanisms also apply encryption to data, they do not provide end-to-end protection. As seen from Figure 1, data is encrypted by VPN and 802.11i when it

travels between the VPN gateway and the wireless client terminal. However, data traveling between the enterprise network and the VPN gateway is transmitted in the clear.

To provide end-to-end protection, applications can encrypt data packets before they are sent out into the network. At the receiving end, the encrypted data will have to be successfully decrypted before the data can be processed. While the encryption and decryption processes are relatively straightforward, the complexity of encryption schemes is in the generation, distribution and management of keys used in the encryption process. Currently, Public Key Infrastructure (PKI) is commonly used in INTERNET and enterprise applications for data encryption and key management. PKI provides strong encryption, as well as strong authentication through digital signing. However, the drawback of PKI is complexity, and it requires the installation of Certificate Authorities (CAs) and other PKI infrastructure in the network.

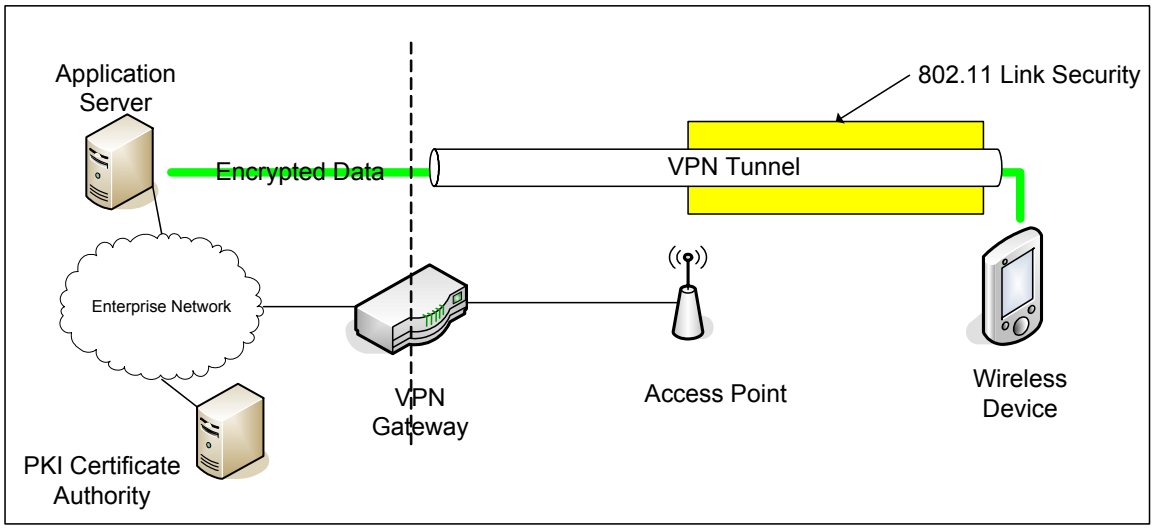

Figure 8. PKI-based Infrastructure

Figure 8 shows the integration of a PKI-based encryption scheme into the wireless architecture. A PKI Certificate Authority is installed within the enterprise network to support the generation of PKI certificates to users in the network. Using this infrastructure, the application server and the wireless device can

encrypt their data and communicate securely end-to-end. The concept of defense in depth is again demonstrated since the encrypted data packets will be further protected by the VPN tunnel and 802.11i mechanisms as they travel between the VPN gateway and the wireless client.

D. MULTI-FACTOR AUTHENTICATION

To provide strong authentication protection, consider the use of multi-factor authentication. Multi-factor authentication adds strength to current authentication mechanisms by adding the attributes of “something you have” to the traditional “something you know” (i.e. passwords) schemes. Examples include smart cards and biometric authentication (e.g. fingerprints or cornea scans).

E. MONITORING

A network monitoring tool should be deployed in the enterprise architecture to monitor and analyze traffic that flows through the wireless network. Deploying a monitoring system is critical for timely detection of probes and attacks, as well as to look out for rogue access points.

Rogue access points are unauthorized access points that are installed in a network. Rogue access points present a risk to the network because they can open up back-door channels for attackers to infiltrate and attack the network. Attackers can also set up access points to masquerade as a legitimate network. When a user attempts to connect to these spoofed networks, the attacker could collect valuable information such as passwords and authenticating materials which is sent by the unsuspecting client.

There are a number of companies that provide monitoring and intrusion detection tools for wireless networks, such as AirDefense, NetworkChemistry and Red-M.

F. DEVICE SECURITY

As computing devices become smaller and more portable, the probability that such devices will be stolen or lost increases substantially. The loss of a device can compromise the security of the enterprise network, since encryption keys and classified information may have been stored on the device.

One potential solution is to apply biometric security, such as fingerprint scanning and recognition onto the mobile devices. An example of a mobile device employing biometric security is the HP IPAQ Pocket PC 5450 shown in Figure 9.

Figure 9. Biometric Protected Device: HP IPAQ Pocket PC 5450 PDA (from[PCWorld 2004])

Biometric protection provides significant improvements to mobile device security. When incorporated with security applications, different levels of protection can be provided to suit the needs of different operating environments. This is an area that should be further investigated. For example, the PDA can be programmed to block access to files stored on the PDA if proper credentials are not supplied, and an administrator is then required to unlock those files. In environments where the loss of the PDA could result in severe operational consequences (such as in a tactical environment), the PDA could even be

programmed to erase all its memory and disks contents via a hard reset in the event of multiple unsuccessful logins.

G. MEDIUM-BASED ACCESS CONTROL

In most traditional systems, the decision to grant or deny access to classified information is typically based on user access rights. However, user access rights do not provide the fine grained controls that may be required by the enterprise's security policy, such as restricting access to classified information from the wireless network.

This section describes an access control mechanism that controls access to information, based on the access medium (i.e. wired or wireless network). This prototype system extends the proof-of concept demonstrator developed in [Nandram 2004]. [Nandram 2004] proposes the use of Extensible Markup Language (XML) tags to differentiate the contents in a particular document based on their security classifications. Based on the user's access rights and the type of access medium, only the relevant sections within the document will be extracted and served to the users.

The concept demonstrator developed in [Nandram 2004] uses the source IP address to determine if the medium of access was a wired or wireless network. However, an IP based scheme requires a segregation of the wireless and wired subnets. An alternative method of determining the medium of access is to use the Medium Access Control (MAC) address. The MAC address is unique to individual networks cards and can be used to identify if it is a wired or wireless network card.

1. Concept of Operation

The concept of operation for the prototype access control mechanism is shown in Figure 10.

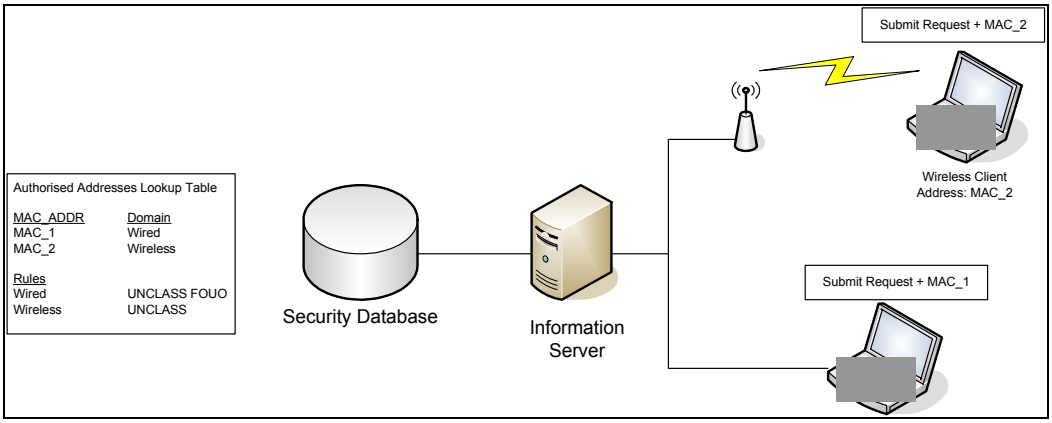

Figure 10. Concept of Operations for Medium-Based Access Control

In Figure 10, the security database look-up table contains the MAC addresses of all authorized network interface cards, as well as the type of the card, i.e. a wired or wireless network card. It also contains the highest security classification of information that the different domains are authorized to carry. In this example, the wired network can carry information up to “UNCLASSIFIED FOR OFFICIAL USE ONLY”, and the wireless network can carry up to “UNCLASSIFIED” information.

When a client requests information from the information server, it has to provide its MAC address to the information server along with the request. On receiving the MAC address, the information server will query the look-up table in the security database to derive information on the medium of access and the classification of information that can be sent. In this illustration, the wireless client will get information content that is rated “UNCLASSIFIED”, and if the same client were to request for the same information on the wired network, the client will receive information content that is rated “UNCLASSIFIED FOR OFFICIAL USE ONLY”. In the event that a submitted MAC address is not found in the security database, the client will be denied information from the server.

2. Implementation and Design

The classes that were implemented for the demonstrator are shown in Figure 11. All software modules implemented were developed using Java.

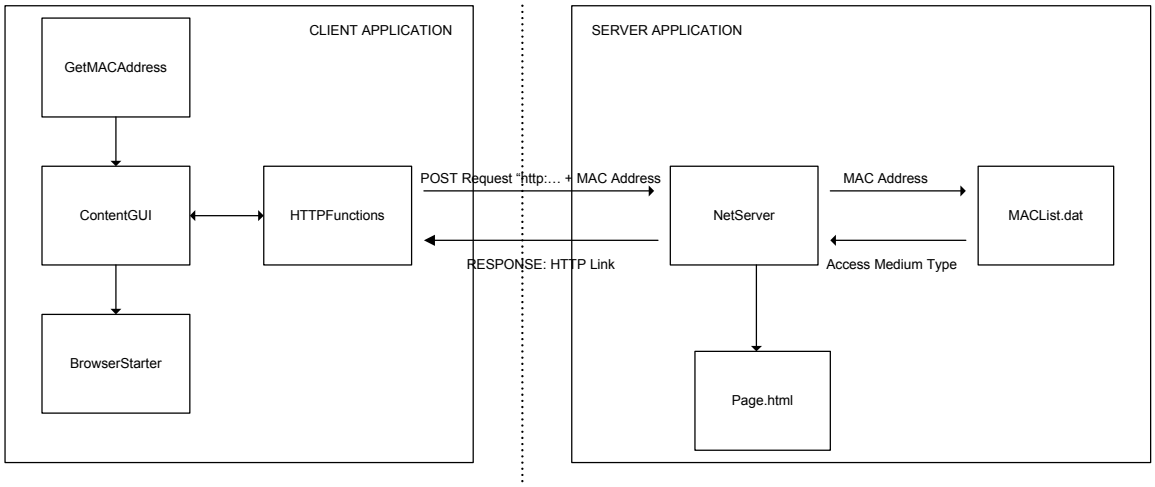

Figure 11. Design Implementation

The design involved software applications on the client end and at the server. For the client application, the key classes are:

- ContentGUI : Provides the graphical user interface for users to invoke requests
- GetMACAddress: Provides functionality to extract the MAC address of the client terminal
- HTTPFunctions: Provide methods to post and receive HTTP requests from the server. A request for a resource is concatenated with the client terminal's MAC address when it is sent to the server. The response that is expected from the server is a HTML link to the requested resource
- BrowserStarter: Used to invoke a browser window to display the returned contents from the server

On the server application, the key classes and files are:

- MACList.dat: This is a simple file that contains a list of registered MAC addresses, and the type of card (i.e. wired or wireless) that is associated with each MAC address
- NetServer: This is a servlet application that listens for requests from users. NetServer extracts out the MAC address of the requesting user and checks it against MACList.dat to determine if the user is on the wired or wireless network. The NetServer class accesses a pre-stored webpage (page.html), and extracts out the relevant contents for the user.
- XMLParser: This class was not implemented due to time and resource constraints. In the current prototype, the parsing was performed by the NetServer servlet.

The source codes for the various classes are listed in Appendix B.

3. Demonstration Program

The Graphical User Interface (GUI) implemented in the ContentGUI class is shown in Figure 12 . The ContentGUI class provides the interface to allow a user to connect to the server and request for pages stored on the server. In this case, the program connects to the NetServer servlet using HTTP function calls, and appends the user terminal's MAC address to the HTTP POST request when the SUBMIT button is pressed.

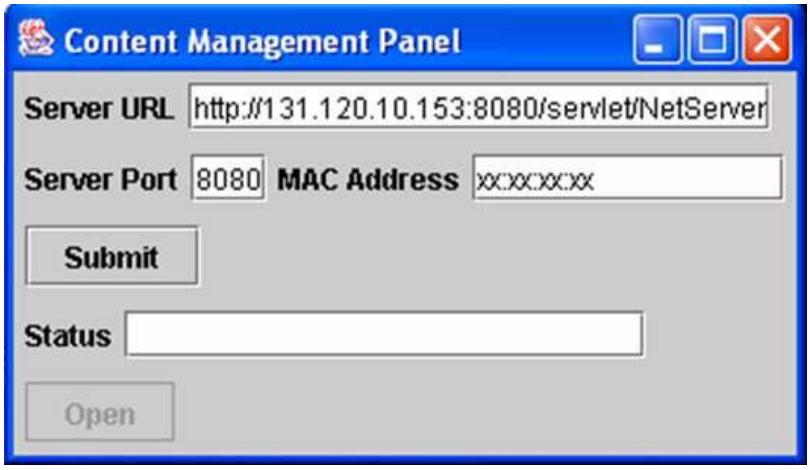

Figure 12, User Graphical Interface

Upon receiving a request, the server will generate the requested information on a web page and return a HTTP link. Invoking the OPEN button will open the web page for viewing on the default web browser the link for browsing by invoking the OPEN button.

Figure 13 shows the view of a web page generated for a user accessing the server via the wired network. In this example, he will be able to see information that is classified up to “UNCLASSIFIED FOR OFFICIAL USE ONLY”.

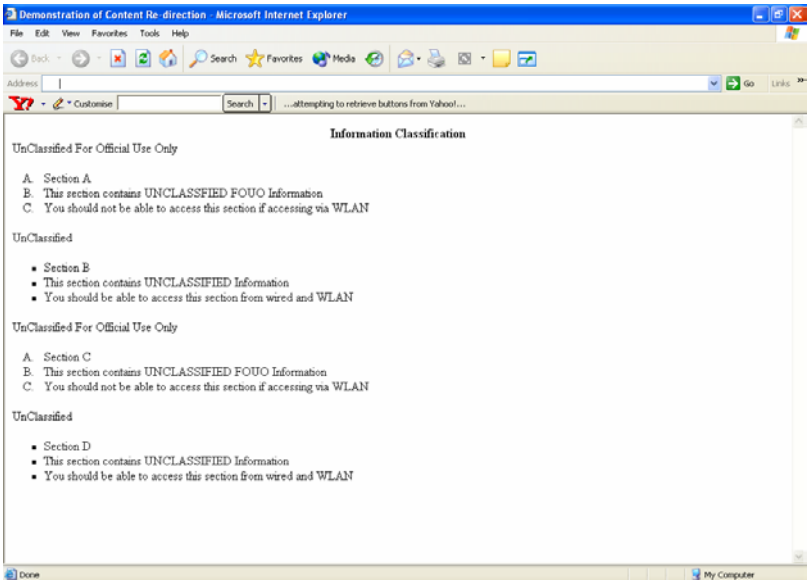

Figure 13. View for User Connected Via the Wired Network

Figure 14 shows the view of the web page generated for a user accessing via the wireless network. In this case, the user is only able to access information up to “UNCLASSIFIED” level.

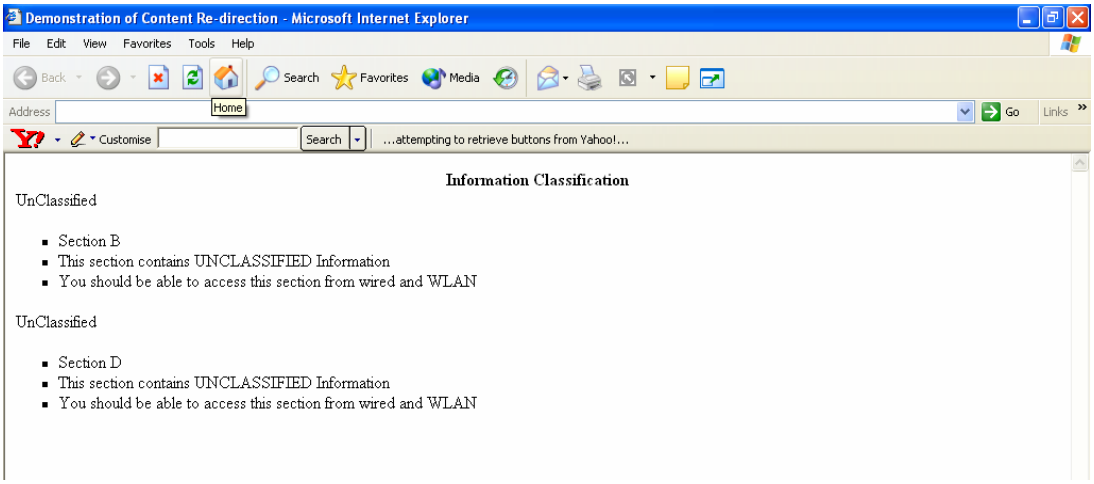

Figure 14. View for User Connected Via the Wireless Network

4. Limitations

In the current prototype, the MAC address is sent to the information server without encryption. This raises a concern that the MAC address can be spoofed and used to gain unauthorized access to the information server. A potential attacker could easily capture the data packets traveling between the client and the server using a simple packet analyzer. Since the MAC address is not encrypted, the attacker could easily extract the MAC address from the captured packets, and modify or replace it with another MAC address. Encryption should therefore be considered to protect the MAC address and prevent spoofing or unauthorized modification.

H. SUMMARY

This chapter outlined a layered-defense strategy that can be adopted to secure the enterprise wireless network. This includes adopting the 802.11i link security protocol, and building additional layers of defense such as including VPNs, encryption and strong authentication. This chapter also recommended the

installation of monitoring tools to monitor the wireless network for suspicious activities and for rogue access points, as well as physical security for mobile devices. Lastly a prototype medium-based access control mechanism was implemented to provide fine grained control of the information that can be accessed from the wireless network.

V. CONCLUSION

A. CONCLUSION

Wireless networks offer the benefits of mobility to the enterprise, but could become a security concern if not properly secured. While wireless networks are inherently less secure then wired networks, a proper security implementation can protect the wireless network sufficiently for it to be used in the enterprise environment.

In this thesis, we studied the problem of implementing a wireless enterprise architecture that meets the specific needs of a DoD enterprise network. A thorough review of the technologies and security implementations pertaining to wireless networks was conducted. The research culminated in the proposal of a layered defense architecture that integrates the various technical solutions into a cohesive defensive mechanism for the enterprise network. The architecture builds on the link layer security mechanisms provided by the IEEE 802.11 standard, and adds additional layers of protection such as VPN and encryption to protect data in transit over the enterprise network. A policy control mechanism was developed that allows a network administrator to control the flow of sensitive information to and from the wireless network.

B. RECOMMENDATIONS AND FURTHER WORK

This thesis provides a basic architecture for implementing a secure WLAN network for DoD specified applications. There is significant room for improvements and additional research. Future work in the following areas is recommended

1. WLAN Security Test Bed

With the conceptual design of the wireless architecture in place, the next step will be to implement the architecture on a test bed system. This system will be useful for testing and evaluating the effectiveness of the various mechanisms proposed in the architecture.

2. Medium-based Access Control Prototype

There are limitations in the current prototype of the medium-based access control system. The current prototype does not provide encryption to protect the MAC address information submitted by the client terminals. Furthermore, the XML framework proposed in [Nandram 2004] was not implemented due to resource and time constraints. Further work is required to develop this tool into a useful access control mechanism. These include

- Integrate application encryption features described in Chapter 4 into the prototype system. This will add security to the communications between the client terminal and the information server.
- Integrate the XML framework into the current prototype. Instead of implementing the file conversion at the servlet application, an XML parser can be used to extract the relevant information from a document and serve it to the client.
- Additional decision rules can be included to further improve on the usefulness of the current prototype. A possible area is to integrate RF-ID tags which track the location of the client terminal in the premises of the enterprise. Based on the location of the client terminal, information with the appropriate security clearance will be sent to that client. This will be useful in enforcing policies which restrict the flow of classified information only in certain rooms or areas in the enterprise.

APPENDIX A. OVERVIEW OF IEEE 802.11 STANDARD

A. OVERVIEW

The IEEE 802.11 standard was first introduced in 1997 to provide wireless networking over limited ranges. The original 802.11 standard operated in the 900 MHz range and provided data rates of up to 2 Mbps. IEEE has since introduced a number of extensions to the 802.11 standard, notably 802.11a, 802.11b, 802.11g. A comparison of the different 802.11 protocols is shown below in Table 7.

	802.11a	802.11b	802.11g
Frequency Band	5GHz UNII	2.4GHz ISM	2.4 GHz ISM
Modulation Scheme	OFDM	DSSS	DSSS or OFDM
Number of Data Channels	12	3	3
Data Rate (Max)	54 Mbps	10 Mbps	54 Mbps
Range	50 m	100 m	100 m
Interoperability	802.11a only	Compatible with 802.11g	Compatible with 802.11b (however, performance will degrade to 802.11b level)

Table 7. Comparison of existing 802.11 Protocols

802.11b is currently the most widely accepted standard among the three standards. The 802.11g was recently ratified in 2003 and is expected to gain a foothold in the market when products supporting 802.11g are released on the market.

B. MODES OF OPERATION

The IEEE 802.11 standard defines 2 basic modes of operations for wireless networking: *infrastructure* and *ad-hoc* mode.

In the infrastructure mode, wireless computer terminals communicate with each other via a wireless access point (AP). The AP coordinates the WLAN and controls the data communications between the wireless terminals. It also provides a bridge between the wired and the wireless network. A typical WLAN system operating in the infrastructure mode is shown in Figure 15 .

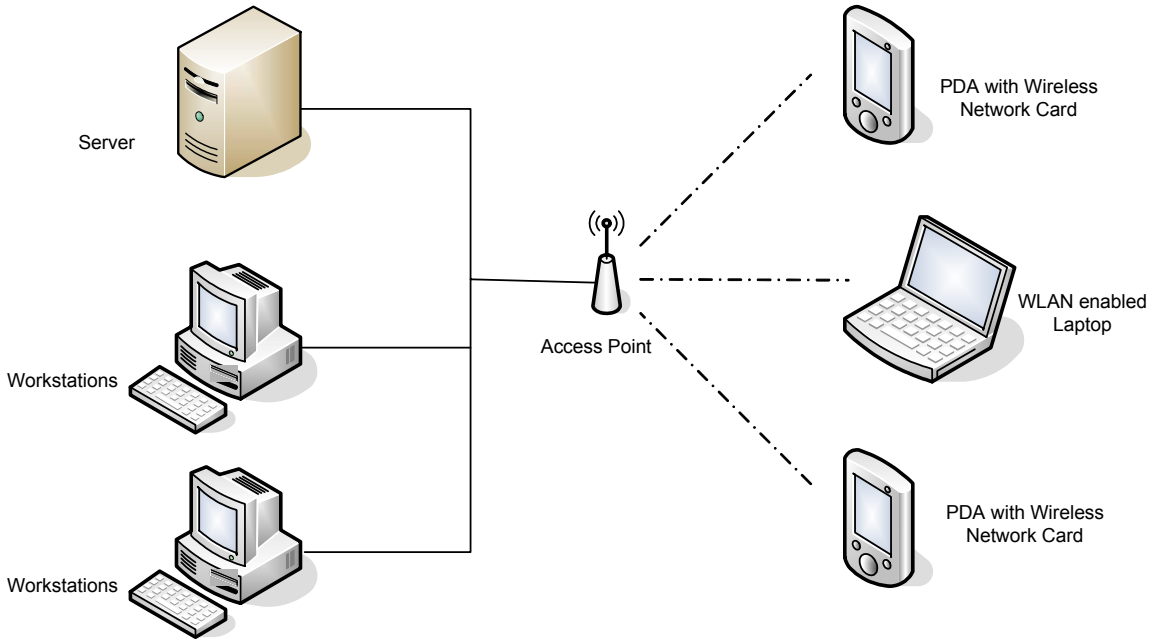

Figure 15. WLAN Operating in Infrastructure Mode

In the ad-hoc mode, the wireless computer terminals communicate directly with each other without the use of an access point. This mode is also commonly known as peer-to-peer mode. The ad-hoc mode provides a simple and easy way for wireless terminals to exchange information without requiring an infrastructure network. A typical ad-hoc network setup is shown in Figure 16.

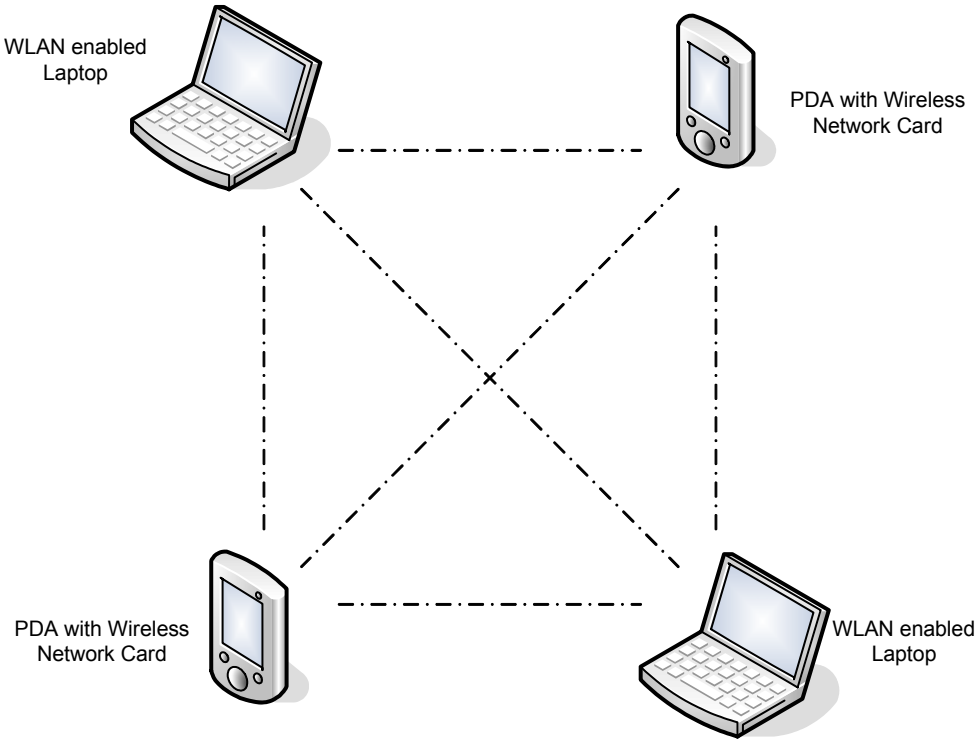

Figure 16. WLAN Operating in Ad-Hoc Mode

C. COLLISION DETECTION AND AVOIDANCE

The 802.11 standard uses the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol to resolve collisions during transmissions. Collisions occur when 2 or more terminals transmit simultaneously while operating in the same channel.

In the CSMA/CA protocol, any terminal that wishes to transmit information is required to sense the medium for any activity. If the medium is busy, the terminal will wait for a period of time before attempting to transmit again. If the medium is free, the source terminal transmits a Request-to-Send (RTS) packet to the destination terminal. On receiving the RTS packet, the receiver terminal will sense the medium and respond with a Clear-to-Send (CTS) packet if the medium is free. The source terminal will start data transmission only when the CTS is received successfully. All other terminals that receive the RTS and CTS messages will defer any transmissions on the medium.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. SOURCE CODES

A. CLIENT APPLICATION MODULE

1. ContentGui.java

```
//*****************************************************
// Name: ContentGui.java
// Purpose: This class implements the GUI portion of the
//          Client Application Module
// Arguments: None
// Output: None
//*****************************************************


import java.lang.*;     // Fundamental class for Java programs
import java.net.*;      // For socket
import java.io.*; // For IOException and Input/OutputStream
import java.util.*;
import java.awt.*;      // Containing classes for user interfaces
import java.awt.event.*;
import javax.swing.*;   // For GUI programming


public class ContentGUI extends JFrame implements ActionListener{

//Text Fields for Server URL, Port Number, Local MAC Address, returned
URL

static private JTextField jtfServerURL, jtfPortNum, jtfMAC, jtfURL;

// Buttons "Submit" - to submit request to server
// Buttin "Open" - to open returned URL link in a new web browser

private JButton jbtSubmit, jbtOpen;

static final int LEFT = 0;
static final int CENTER = 1;
static final int RIGHT = 2;

// default string values for the test fields

static final String strServerURL =
"http://131.120.10.153:8080/servlet/NetServer";
static final String strPortNum = "8080";
static final String DELIMITER = "%";
```

```
public ContentGUI () {

       setTitle("Content Management Panel");

       //*************************************************************
       // Create the panels
       //*************************************************************

       JPanel p1 = new JPanel();
       p1.setLayout(new FlowLayout(LEFT));
       p1.add(new JLabel("Server URL"));
       p1.add(jtfServerURL = new JTextField(strServerURL));


       JPanel p2 = new JPanel();
       p2.setLayout(new FlowLayout(LEFT));
       p2.add(new JLabel("Server Port"));
       p2.add(jtfPortNum = new JTextField(strPortNum));
       p2.add(new JLabel("MAC Address"));
       p2.add(jtfMAC = new JTextField(12));


       JPanel p3 = new JPanel();
       p3.setLayout(new FlowLayout(LEFT));
       p3.add(jbtSubmit = new JButton("Submit"));


       JPanel p4 = new JPanel(new BorderLayout());
       p4.add(p1, BorderLayout.NORTH);
       p4.add(p2, BorderLayout.CENTER);
       p4.add(p3, BorderLayout.SOUTH);


       JPanel p5 = new JPanel();
       p5.setLayout(new FlowLayout(LEFT));
       p5.add(new JLabel("Status"));
       p5.add(jtfURL = new JTextField(20));

       JPanel p6 = new JPanel();
       p6.setLayout(new FlowLayout(LEFT));
       p6.add(jbtOpen = new JButton("Open"));
       jbtOpen.setEnabled(false);

       //Register listeners

       jbtSubmit.addActionListener(this);
       jbtOpen.addActionListener(this);
```

```
        //************************************************************
        // Add panels to the frame
        //************************************************************
        getContentPane().setLayout(new BorderLayout());
        getContentPane().add (p4, BorderLayout.NORTH);

        getContentPane().add (p5, BorderLayout.CENTER);

        getContentPane().add (p6, BorderLayout.SOUTH);
}


public static void main(String[] args) throws IOException {

        ContentGUI frame = new ContentGUI();
        frame.setDefaultCloseOperation(JFrame.EXIT_ON_CLOSE);
        frame.pack();
        frame.setVisible(true);

        String strMAC;
        GetMacAddress gMac = new GetMacAddress();
        strMAC = gMac.getMac();
        jtfMAC.setText(strMAC);

}


public void actionPerformed(ActionEvent e){

String strSubmitURL, strData, strReply;

String actionCommand = e.getActionCommand();
HTTPFunctions hConn = new HTTPFunctions();
//Handle button events

if(e.getSource() instanceof JButton){

        if ("Submit".equals(actionCommand)){
        strSubmitURL = jtfServerURL.getText();
        strData = jtfMAC.getText();
        try{
        strReply = hConn.PostRequest(strSubmitURL, strData);

        if (strReply.compareToIgnoreCase("Invalid MAC Address")== 0)
              jtfURL.setText(strReply);
              else{
              jtfURL.setText(strReply);
              jbtOpen.setEnabled(true);
              }
        }catch(Exception err){}

        }


        if ("Open".equals(actionCommand)){
```

```
      String str = jtfURL.getText();
      try{
      BrowserStarter bb = new BrowserStarter();
      bb.openURL("http://131.120.10.153/out.html");
      jbtOpen.setEnabled(false);
      }catch(Exception err){}
      }

}
}
            } // end class
```

2. GetMACAddress.java

```
//*****************************************************
// Name: GetMacAddress.java
// Purpose: Class that retrieves the MAC address of the
//          local host terminal
// Arguments: None
// Output: Returns MAC address as a string
//*****************************************************

import java.io.BufferedInputStream;
import java.io.IOException;
import java.io.*;
import java.util.*;


public class GetMacAddress {

public GetMacAddress(){}            //constructor


public String getMac(){

String []cmd = {"cmd.exe","/c","ipconfig /all"};
String output = "";
String MAC_Address = "";
try {
Process ps = Runtime.getRuntime().exec(cmd);
int ptr = 0;
InputStream in;
in = new BufferedInputStream(ps.getInputStream());
StringBuffer buffer = new StringBuffer();
while( (ptr = in.read()) != -1 ) {
buffer.append((char)ptr);
}
output =  buffer.toString();



StringTokenizer st = new StringTokenizer(output,"\n");
int i=1;
String line="";
//String MAC_Address = "";
```

```
while(st.hasMoreTokens()){
line= st.nextToken();

//System.out.println(line);

if (line.trim().startsWith("Ethernet"))
{
line = st.nextToken();
System.out.println(line);

line = st.nextToken();

      if (line.trim().startsWith("Media State")){
      line= st.nextToken();
      line= st.nextToken();
      line= st.nextToken();
      }

}

if (line.trim().startsWith("Physical Address"))
{

MAC_Address = line.trim();
StringTokenizer st1 = new StringTokenizer(MAC_Address,":");
st1.nextToken();
MAC_Address = st1.nextToken();
MAC_Address = MAC_Address.trim();


break;
}
//System.out.println("Token "+(i++)+":"+ line);
}
//System.err.print(loadStream(ps.getErrorStream()));
} catch(IOException ioe) {
ioe.printStackTrace();
}

return MAC_Address;
}
}
```

\

3. HTTPFunctions.java

```
//*********************************************************************
//Name: HTTPFunctions.java
//Purpose:  Provide methods for applications to invoke HTTP Post
          and Get functions
//*********************************************************************

import java.net.*;
import java.io.*;
import java.util.*;


public class HTTPFunctions {

public HTTPFunctions(){}            //constructor

public String PostRequest( String strURL, String data) throws
MalformedURLException, IOException, IllegalStateException


{
// generic function to send a post request to the server.
String strOut = "";
URL url = new URL(strURL);
HttpURLConnection connection = (HttpURLConnection)url.openConnection();
connection.setRequestMethod("POST");
connection.setDoOutput(true);

PrintWriter out = new PrintWriter(connection.getOutputStream());
out.print(data);
out.close();

BufferedReader in = new BufferedReader(new
InputStreamReader(connection.getInputStream()));

//Read the return text only if the response is OK

if (connection.getResponseCode() == HttpURLConnection.HTTP_OK)
      {
            String line;
            while ((line = in.readLine()) != null)
            {
                  strOut = line;
            }
      }

in.close();
return(strOut);
}

}
```

B. SERVER SIDE APPLICATIONS

1. NetServer.java

```
// ************************************************************
// Name: NetServer.java
// Purpose: Implements a servlet application that accepts HTTP
//          Post requests from clients
//          This servlet extracts out the MAC address that is
//          appended with the HTTP post request
//          Based on the MAC address, the servlet extracts out
//          the relevant information from the template information
//          file page.html and stores the relevant content in
//          new HTML file out.html
//          The client is returned the URL link to out.html
//************************************************************

import java.lang.*;
import java.util.*;
import java.io.*;
import javax.servlet.*;
import javax.servlet.http.*;

public class NetServer extends HttpServlet {

//GetMacType gType = new GetMacType();

private String processData(char[] inData) {
                String s = new String(inData);
                StringBuffer sb = (new StringBuffer(s)).reverse();
                return  sb.toString();
        }

public String Extract(String CLASSIFICATION , String File_Name){

BufferedReader infile = null;
FileReader frs = null;
FileWriter fws = null;
PrintWriter out = null;
String strTemp;

try   {
      frs = new FileReader(   File.separator + "var" + File.separator +
                              "www" + File.separator + "html" +
                              File.separator +  File_Name);

      infile = new BufferedReader(frs);

      fws = new FileWriter(   File.separator + "var" + File.separator +
                              "www" + File.separator+ "html" +
                              File.separator  +  "out.html");


      out = new PrintWriter(fws);

      boolean blnWriteCurrentLine = true;
```

```
      while ((strTemp = infile.readLine()) != null)
      {
            // gets rid of the <low> and </low> tags
            if
((strTemp.trim().startsWith("<low>"))||(strTemp.trim().startsWith("</lo
w>")))
            strTemp = infile.readLine();

            // Removes high classification content if Access right is
low

            if (strTemp.trim().startsWith("<high>")){

                  if(CLASSIFICATION.compareToIgnoreCase("low")==0)
                  blnWriteCurrentLine = false;

                  if(CLASSIFICATION.compareToIgnoreCase("high")==0)
                  blnWriteCurrentLine = true;
                  String str = "";

                  strTemp = infile.readLine();
                  do{

                  str = str + strTemp;
                  strTemp = infile.readLine();

                  }while(!(strTemp.trim().startsWith("</high>")));
                  strTemp = str;
                  //while (!(strTemp.trim().startsWith("</high>"))){
                  //strTemp = infile.readLine();
                  //}




            }

      if (blnWriteCurrentLine)
      out.println(strTemp);

      blnWriteCurrentLine = true;
      }
}
catch(FileNotFoundException ex){}
catch(IOException ex){}
finally{
      try {
      if (frs !=null) frs.close();
      if (fws !=null) fws.close();
      }catch(IOException ex){}
}
return("");
}
```

```
public String getMACType(String MAC_ADDR , String File_Name){

BufferedReader infile = null;
FileReader frs = null;
StringTokenizer st;
String strTemp;
String strType = "UNK";
String strMac;
int intType = 0;
int IntCount = 0;

try   {
      frs = new FileReader(File.separator + File_Name);
      infile = new BufferedReader(frs);

      while ((strTemp = infile.readLine()) != null)
      {

      st = new StringTokenizer(strTemp, "\t");
      strMac = st.nextToken();
      System.out.println(strMac);
      if (strMac.compareToIgnoreCase(MAC_ADDR)==0)
            {
                  strType = st.nextToken();
                  break;
            }
      }
}
catch(FileNotFoundException ex){}
catch(IOException ex){}
finally{
      try {
      if (frs !=null) frs.close();
      }catch(IOException ex){}
}


return (strType);
}

        // used to test this servlet.
public void doGet(HttpServletRequest request,
HttpServletResponse response) throws IOException, ServletException {
      PrintWriter out = response.getWriter();
      response.setContentType("text/plain");
      out.write("The NetServer Servlet is working");
      out.flush();
      }
```

```
    //**
    // * Respond to a POST request for the content produced by
    // * this servlet.
    // *
    // * @param request The servlet request we are processing
    // * @param response The servlet response we are producing
    // *
    // * @exception IOException if an input/output error occurs
    // * @exception ServletException if a servlet error occurs
    // *//

public void doPost(HttpServletRequest request,HttpServletResponse
response) throws IOException, ServletException {

      Date date = new Date();
      BufferedReader reader = request.getReader();
      char inData[] = new char[request.getIntHeader("Content-Length")];
      reader.read(inData, 0, inData.length);

      StringBuffer sb = new StringBuffer();

      sb.append("NetServer Servlet\r");
      sb.append(date.toString() + "\r");
      sb.append(new String(inData) + "\r");


      String strMAC = new String(inData);
      String strVal = getMACType(strMAC, "MACList.dat");

      if (strVal.compareToIgnoreCase("WIRELESS")==0)
      {strVal = Extract("low", "page.html");

      sb.append("http://131.120.10.153/out.html" + "\r");
      }else if (strVal.compareToIgnoreCase("WIRED")==0)

            {strVal = Extract("high", "page.html");
            sb.append("http://131.120.10.153/out.html" + "\r");
            }else
            sb.append("Invalid MAC Address" + "\r");

            response.setContentType("text/plain");
            response.setContentLength(sb.length());

            PrintWriter out = response.getWriter();
            out.write(sb.toString());
            out.flush();
        }
}
```

2. Sample Content Page (Page.html)

```
<html>
<head>
<title> Demonstration of Content Re-direction</title>
</head>

<body bgcolor=white>
<center><b>Information Classification</b></center>
<high>
UnClassified For Official Use Only
<ol type=A>
      <li> Section A
      <li> This section contains UNCLASSFIED FOUO Information
      <li> You should not be able to access this section if accessing
via WLAN
</ol>
</high>
<low>
UnClassified
<ul type=square>
      <li> Section B
      <li> This section contains UNCLASSIFIED Information
      <li> You should be able to access this section from wired and
WLAN
</ul>
</low>
<high>
UnClassified For Official Use Only
<ol type=A>
      <li> Section C
      <li> This section contains UNCLASSIFIED FOUO Information
      <li> You should not be able to access this section if accessing
via WLAN
</ol>
</high>
<low>
UnClassified
<ul type=square>
      <li> Section D
      <li> This section contains UNCLASSIFIED Information
      <li> You should be able to access this section from wired and
WLAN
</ul>
</low>
</body>
</html>
```

3. Output Page Generated for Client on Wireless Network

```
<html>
<head>
<title> Demonstration of Content Re-direction</title>
</head>

<body bgcolor=white>
<center><b>Information Classification</b></center>
UnClassified
<ul type=square>
      <li> Section B
      <li> This section contains UNCLASSIFIED Information
      <li> You should be able to access this section from wired and
WLAN
</ul>
UnClassified
<ul type=square>
      <li> Section D
      <li> This section contains UNCLASSIFIED Information
      <li> You should be able to access this section from wired and
WLAN
</ul>
</body>
</html>
```

4. Output Page Generated for Client on Wired Network

```
<html>
<head>
<title> Demonstration of Content Re-direction</title>
</head>

<body bgcolor=white>
<center><b>Information Classification</b></center>
UnClassified For Official Use Only
<ol type=A>
      <li> Section A
      <li> This section contains UNCLASSFIED FOUO Information
      <li> You should not be able to access this section if accessing
via WLAN
</ol>
UnClassified
<ul type=square>
      <li> Section B
      <li> This section contains UNCLASSIFIED Information
      <li> You should be able to access this section from wired and
WLAN
</ul>
UnClassified For Official Use Only
<ol type=A>
      <li> Section C
      <li> This section contains UNCLASSIFIED FOUO Information
      <li> You should not be able to access this section if accessing
via WLAN
</ol>
UnClassified
<ul type=square>
      <li> Section D
      <li> This section contains UNCLASSIFIED Information
      <li> You should be able to access this section from wired and
WLAN
</ul>
</body>
</html>
```

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[NIST 2002] Tom Karygiannis and Les Owens. "Wireless Network Security-802.11, Bluetooth and Handheld Devices". Special Publication 800-48, National Institute of Standards and Technology, sections 1 – 3, Nov 2002.

[DCID 6/3 1999] Director of Central Intelligence Agency Directive No 6/3. "Protecting Sensitive Compartmented Information within Information Systems.", Central Intelligence Agency, Jun 1999.

[DCID 6/9 2002] Director of Central Intelligence Agency Directive No 6/9. "Physical Security Standards for Sensitive Compartmented Information Facilities", Central Intelligence Agency, 18 Nov 2002.

[Bersani 2004] Bersani, "EAP Shared Key Methods: A Tentative Synthesis of Those Proposed So Far" http://ietfreport.isoc.org/idref/draft-bersani-eap-synthesis-sharedkeymethods/ date accessed 26 Nov 2004, Internet Engineering Task Force, April 2004.

[Borisov 2002] Nikita Borisov, Ian Goldberg, David Wagner, " Intercepting Mobile Communications: The Insecurity of 802.11-Draft". http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf] date accessed 23 Sep 2004.

[Edney & Arbaugh 2004] Jon Edney and William A. Arbaugh. "Real 802.11 Security, WiFi Protected Access and 802.11i". Addison Wesley 2004.

[FIPS 197 2001] Federal Information Processing Standards Publication 197, "Announcing the Advanced Encryption Standard (AES)", http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf, date accessed 26 Nov 2004.

[CNSS 2003] "CNSS Policy No. 15, Fact Sheet No. 1 National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information", http://www.nstissc.gov/Assets/pdf/fact%20sheet.pdf date accessed 26 Nov 2004, CNSS, Jun 2003.

[Kaufman 2002] Charlie Kaufman, Radia Perlman and Mike Speciner. "Network Security, Private Communications in a Public World", 2nd Edition, p 104, Prentice Hall, 2002.

[PCWorld 2004]
http://www.pcworld.com/reviews/article/0,aid,108240,src,ov,00.asp date accessed 26 Nov 2004, PCWorld, Nov 2004.

[Nandram 2004] Nandram, W. “Information Security and Wireless: Alternate Approaches for Controlling Access to Critical Information”, Thesis, Naval Postgraduate School, 2004.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Professor Karen Burke
   Naval Postgraduate School
   Monterey, California

4. Professor Gurminder Singh
   Naval Postgraduate School
   Monterey, California

5. Oh Khoon Wee
   Defense Science & Technology Agency (DSTA)
   Singapore